

IPX-AES

Symmetric Security Range

AES SYMMETRIC SECURITY RANGE

The IPX-AES Module is an encryptor / decryptor core range that efficiently implements in FPGA the Advanced Encryption Standard as specified in the Federal Information Processing publication FIPS-197 of the National Institute of Standards and Technology.

The IPX-AES module can be customized to ensure its optimization for a wide range of specific applications with a design architecture that can be adapted to support from low up to very high bit-rates. Its flexibility allows combining several functions and operating modes on very small footprints.

■ All AES options available

■ Multiple Stream Management

■ Bypass mode

■ Renewable security

THE intoPIX PLUS ...

✓ Efficient FPGA footprint

✓ Flexible architecture

✓ Field upgradeable

✓ Customizable

✓ High bitrate capable



intoPIX s.a.
Place de l'Université 16
B-1348 Louvain-la-Neuve
Tel.: +32 (0)10 23 84 70

www.intopix.com

FEATURE	OPTIONS
AES Data and Key sizes	<ul style="list-style-type: none"> • 128 bits • 256 bits
Functions	<ul style="list-style-type: none"> • Decryption • Encryption • Encryption-Decryption • Bypass
Data-stream handling	<ul style="list-style-type: none"> • Single stream • Multiple streams
Operation modes	<ul style="list-style-type: none"> • ECB • CBC • CTR • CFB • OFB
Data and key bus widths	<ul style="list-style-type: none"> • 32 bits • 128 bits • 256 bits
Signal clock with asynchronous reset	<ul style="list-style-type: none"> • 1
Simple external interface	<ul style="list-style-type: none"> • Yes
Modules	<ul style="list-style-type: none"> • Looped • Unrolled
Pipelined	<ul style="list-style-type: none"> • Pipelined • Un-Pipelined
Bit rate	<ul style="list-style-type: none"> • From 350 Mbit/s up to 20 Gbit/s

FUNCTIONS

Addressing keys of 128 or 256 bits, the IPX-AES cores execute decryption only, encryption only, a combination of encryption and decryption functions plus a bypass mode.

DATA-STREAM HANDLING

The IPX-AES cores can handle the data and secret keys in two different ways.

- The Single Stream option consists of a core capable to encrypt/decrypt data with a single key, before a new update of this key.
- The Multiple Stream option is a feature capable to manage multiple ciphering processes together, each based on a different secret key.

CHAINING MODES

The inter-data-block chaining supports all existing modes that can be used separately or combined into a single design: ECB (Electronic Code-Book), CBC (Cipher Block Chaining), CTR (Counter), CFB (Cipher Feedback), and OFB (Output Feedback).

DATA BUSES

The incoming, outgoing and key data are handled on either common or separate buses. Data bus width can be sized 32, 128 or 256 bits wide.

Bus splitting between data stream, key and initialization value enables high bitrate operations.

CLOCK

The processes use a single clock and can be reset asynchronously. They may be pipelined, looped or unrolled.

INSTRUCTION SET

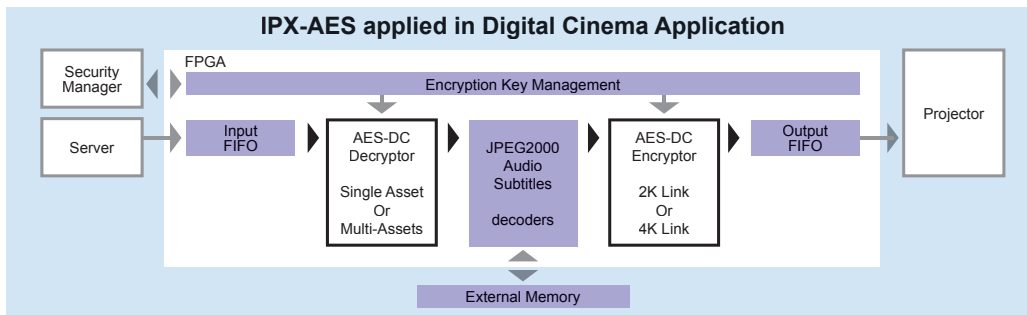
The whole process is controlled by a simple set of instructions.

IPX-AES

Symmetric Security Range

EXAMPLE: DIGITAL CINEMA MODULES

IPX-AES-L DC 250Mbps Asset Decryptor
IPX-AES-MD DC 1Gbps Multi-Asset Decryptor
IPX-AES-M DC 2K Link Encryptor
IPX-AES-H DC 4K Link Encryptor



These four versions of the IPX-AES are designed specifically to meet Digital Cinema needs, and demonstrate how powerful and efficient IPX-AES can be.

The modules specified are intended for use in Xilinx FPGAs and comply with the Digital Cinema Initiative Requirement Specification V1.1.

In particular, as illustrated, the IPX-AES-L can be used to decrypt a single asset at up to 250 Mbps (e.g. picture, audio or subtitles).

The IPX-AES-MD can manage multiple assets simultaneously at more than 1 Gbps with automatic context swap between de-

ryption processes. Furthermore, while handling mix of encrypted and in-clear asset data, the core maintains a consistent processing delay between the decryption and bypass modes.

The IPX-AES-M and the IPX-AES-H can be used to re-encrypt respectively 2K and 4K uncompressed data between the Media-Block and the projector.

And, thanks to the compactness of the intoPIX IP-core, it is possible to combine asset decryption, JPEG 2000 decoding, picture watermarking and local link encryption in a single and affordable FPGA.

DIGITAL CINEMA APPLICATIONS

DC requirement

- ✓ 128 bit Key
- ✓ CBC Mode
- ✓ Asset Decryption
- ✓ Local Link Encryption

THE intoPIX PLUS ...

- ✓ Multiple Asset Decryption in a single IP-core
- ✓ 1Gbps Asset Decryption
- ✓ Full picture processing chain in a single FPGA

IPX-AES	DC-250Mbps-ASSET DECRYPTOR	DC-1Gbps-MULTI-ASSETS DECRYPTOR	DC-2K LINK-ENCRYPTOR	DC-4K LINK-ENCRYPTOR
AES Data and Key size	128 bits	128 bits	128 bits	128 bits
Function	Decryption only	Decryption & Bypass	Encryption only	Encryption only
Data-stream handling	Single stream	Multiple stream	Single stream	Single stream
Operation mode	CBC	CBC	CTR	CTR
Data and key bus width	32 bits	128 bits	128 bits	128 bits
Synthesized on	Virtex-4 SX35-10	Virtex-4 SX35-10	Virtex-4 SX35-10	Virtex-4 SX35-10 Virtex-4 FX60-10
Slices	300	1300	750	3000
RAM Block	3	8	10	40
Work Frequency	125 MHz	200 MHz	250 MHz	250 MHz
Encryption/decryption cycle count	44 cycles	11 clock cycles	11 clock cycles	11 clock cycles
Encryption throughput	363 Mbit/s	2,3 Gbit/s	3 Gbit/s	12 Gbit/s
Key update cycle count	92 cycles	34 cycles	On the fly	On the fly



intoPIX s.a.
 Place de l'Université 16
 B-1348 Louvain-la-Neuve
 Tel.: +32 (0)10 23 84 70

www.intopix.com

Information provided is accurate at the time of publication, however, no responsibility is assumed by intoPIX for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implication or otherwise under any patent or patent rights of intoPIX. Trademarks and registered trademarks are the property of their respective owners.